Private-Key Cryptography

CS 276: Introduction to Cryptography

Sanjam Garg

February 11, 2026

Overview

1. Private-Key Encryption
2. Security Definitions
3. CPA-Secure Encryption from PRF
4. Counter Mode

Setting

Goal

Alice and Bob want to communicate. Only Alice sends a message to Bob. No **eavesdropper** should learn the message.

Setting

Goal

Alice and Bob want to communicate. Only Alice sends a message to Bob. No **eavesdropper** should learn the message.

Protocol

1. **Key generation**: Alice and Bob agree on a key k (only they know it).
2. **Encrypt**: Alice computes ciphertext $c \leftarrow \mathrm{Enc}(k, m)$ and sends c to Bob.
3. **Decrypt**: Bob recovers $m \leftarrow \mathrm{Dec}(k, c)$.

Setting

Goal

Alice and Bob want to communicate. Only Alice sends a message to Bob. No **eavesdropper** should learn the message.

Protocol

1. **Key generation**: Alice and Bob agree on a key k (only they know it).
2. **Encrypt**: Alice computes ciphertext $c \leftarrow \mathrm{Enc}(k, m)$ and sends c to Bob.
3. **Decrypt**: Bob recovers $m \leftarrow \mathrm{Dec}(k, c)$.

Requirements

Correctness: Decryption recovers the message. **Confidentiality**: Eavesdropper learns nothing about m from c. (We may also want *integrity* and *authenticity*.)

Private-Key Encryption Scheme

Definition 1 (Private-Key Encryption Scheme)

A **private-key encryption scheme** Π is a tuple $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$:

1. $\mathsf{Gen}(1^n) \to k$ (key generation)
2. $\mathsf{Enc}(k, m) \to c$ (encryption)
3. $\mathsf{Dec}(k, c) \to m'$ (decryption)

where n is the security parameter and $k, c, m, m' \in \{0, 1\}^*$.

Correctness

Definition 2 ((Perfect) Correctness)

$\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is **(perfectly) correct** if for all n, all k output by $\mathsf{Gen}(1^n)$, and all $m \in \{0,1\}^*$:

$$\Pr[\mathsf{Dec}(k, \mathsf{Enc}(k, m)) = m] = 1$$

For fixed-length schemes we require $m \in \{0,1\}^{\ell(n)}$ for a polynomial $\ell(n)$.

IND Security (Weak)

Definition 3 (IND Security)

Π satisfies **IND security** if for all m_0, m_1 with $|m_0| = |m_1| = \ell(n)$, and all non-uniform PPT $\mathcal{A}$:

$$\left| \Pr[\mathcal{A}(1^n, \mathsf{Enc}(k, m_b)) = b] - \frac{1}{2} \right| = \mathsf{negl}(n)$$

where $k \leftarrow \mathsf{Gen}(1^n)$ and probability is taken over the random choice of k, Enc, b.

IND Security (Weak)

Definition 3 (IND Security)

Π satisfies **IND security** if for all m_0, m_1 with $|m_0| = |m_1| = \ell(n)$, and all non-uniform PPT $\mathcal{A}$:

$$\left|\Pr[\mathcal{A}(1^n, \mathsf{Enc}(k, m_b)) = b] - \frac{1}{2}\right| = \mathsf{negl}(n)$$

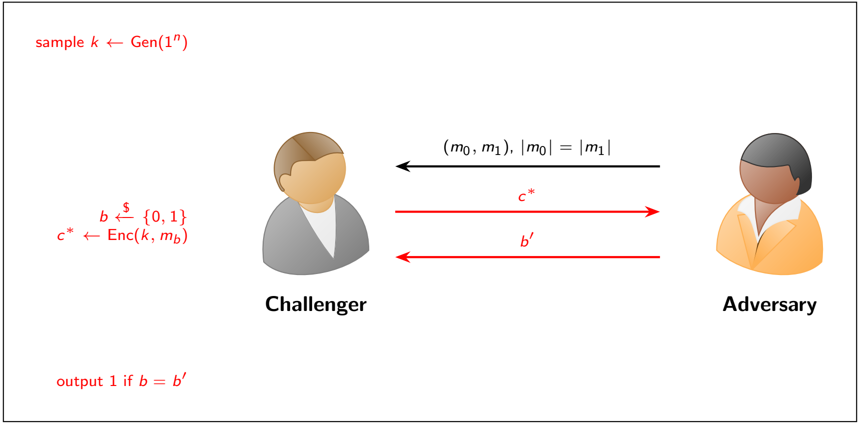
where $k \leftarrow \mathsf{Gen}(1^n)$ and probability is taken over the random choice of k, Enc, b.

Limitation

The attacker only sees one ciphertext and must guess which of m_0 or m_1 was encrypted. No oracle access. Too weak for practice.

IND Security (Weak): Challenger vs Adversary

$$\mathsf{IND}_{\Pi}^{\mathcal{A}}(n)$$



IND Security

Definition 4 (CPA Security)

Π is **IND-secure** if for all non-uniform PPT $\mathcal{A}$:

$$\mathsf{Adv}^{\mathsf{IND}}_{\Pi,\mathcal{A}}(n) = \left| \Pr[\mathsf{IND}^{\mathcal{A}}_{\Pi}(n) = 1] - \frac{1}{2} \right| = \mathsf{negl}(n)$$

CPA Security: The Game

Game IND-CPA$_\Pi^\mathcal{A}(n)$

1. $b \xleftarrow{\$} \{0,1\}$; $k \leftarrow \mathsf{Gen}(1^n)$
2. $\mathcal{A}$ gets oracle $\mathsf{Enc}(k,\cdot)$; outputs (m_0, m_1) with $|m_0| = |m_1|$
3. Challenger gives $c^* \leftarrow \mathsf{Enc}(k, m_b)$ to $\mathcal{A}$
4. $\mathcal{A}$ again gets $\mathsf{Enc}(k,\cdot)$; outputs b'
5. Output 1 iff $b' = b$ (and $|m_0| = |m_1|$)

CPA Security: The Game

Game IND-CPA$_{\Pi}^{\mathcal{A}}(n)$

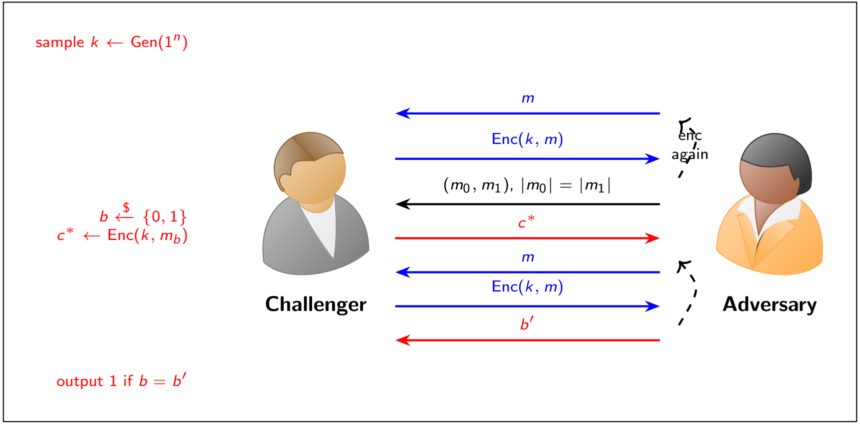
1. $b \xleftarrow{\$} \{0,1\}$; $k \leftarrow \mathsf{Gen}(1^n)$
2. $\mathcal{A}$ gets oracle $\mathsf{Enc}(k,\cdot)$; outputs (m_0, m_1) with $|m_0| = |m_1|$
3. Challenger gives $c^* \leftarrow \mathsf{Enc}(k, m_b)$ to $\mathcal{A}$
4. $\mathcal{A}$ again gets $\mathsf{Enc}(k,\cdot)$; outputs b'
5. Output 1 iff $b' = b$ (and $|m_0| = |m_1|$)

Key point

The key k is sampled **before** $\mathcal{A}$ chooses m_0, m_1. So oracle access to $\mathsf{Enc}(k,\cdot)$ is meaningful.

IND-CPA: Challenger vs Adversary

$$\text{IND-CPA}_{\Pi}^{\mathcal{A}}(n)$$



CPA Security

Definition 5 (CPA Security)

Π is **CPA-secure** (Chosen Plaintext Attack secure) if for all non-uniform PPT $\mathcal{A}$:

$$\mathsf{Adv}^{\mathsf{CPA}}_{\Pi,\mathcal{A}}(n) = \left| \Pr[\mathsf{IND\text{-}CPA}^{\mathcal{A}}_{\Pi}(n) = 1] - \frac{1}{2} \right| = \mathsf{negl}(n)$$

IND vs CPA: Why Order Matters

Example: IND-secure but not CPA-secure

- $\mathsf{Gen}'(1^n)$: run $k \leftarrow \mathsf{Gen}(1^n)$, $x \overset{\$}{\leftarrow} \{0,1\}^n$, output $k' = (k, x)$
- $\mathsf{Enc}'(k', m)$: if $m = x$ output x; else output $\mathsf{Enc}(k, m) \| x$

IND vs CPA: Why Order Matters

Example: IND-secure but not CPA-secure

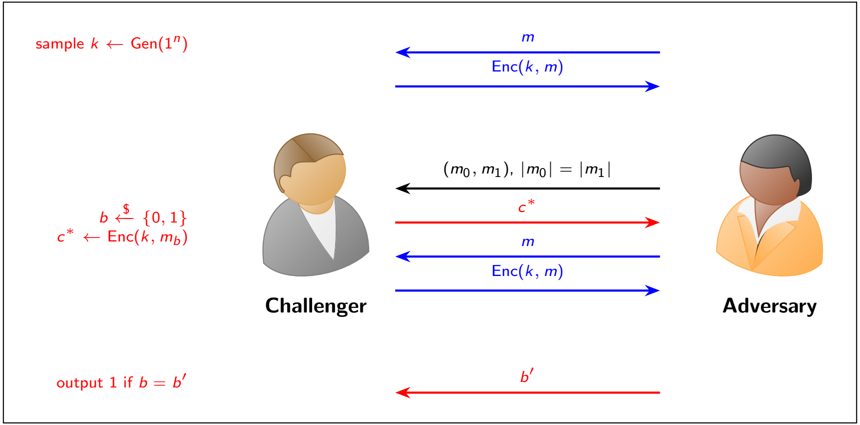
- $\mathrm{Gen}'(1^n)$: run $k \leftarrow \mathrm{Gen}(1^n)$, $x \xleftarrow{\$} \{0,1\}^n$, output $k' = (k, x)$
- $\mathrm{Enc}'(k', m)$: if $m = x$ output x; else output $\mathrm{Enc}(k, m) \| x$

Attack

Adversary queries $\mathrm{Enc}(k', \cdot)$ on many messages. Eventually gets $c = x$ when $m = x$. Then can use x to break indistinguishability. With IND, m_0, m_1 fixed before k; oracle doesn't help.

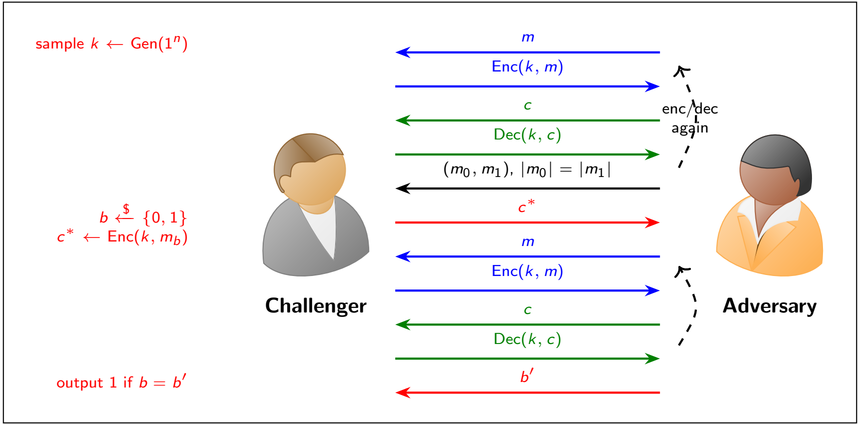
CCA Security: Challenger vs Adversary

$\text{IND-CCA}_{\Pi}^{\mathcal{A}}(n)$



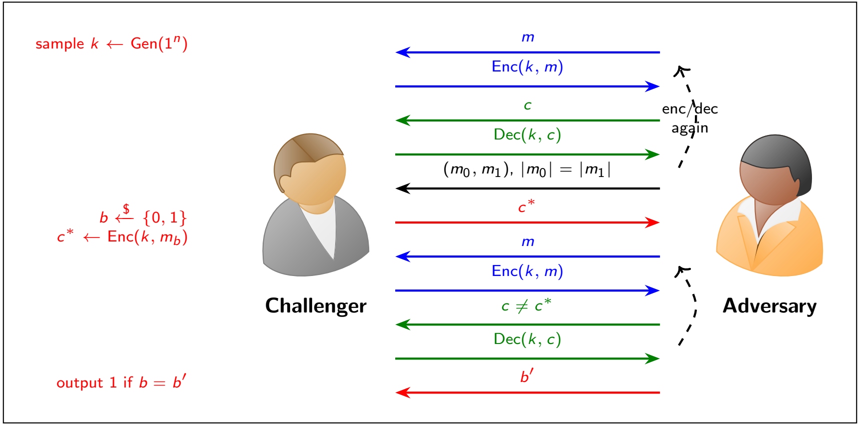
CCA Security: Challenger vs Adversary

$\text{IND-CCA}_{\Pi}^{\mathcal{A}}(n)$



CCA Security: Challenger vs Adversary

$$\text{IND-CCA}_{\Pi}^{\mathcal{A}}(n)$$



CCA Security

Game IND-CCA$_\Pi^\mathcal{A}(n)$

Challenger picks $b \xleftarrow{\$} \{0,1\}$, $k \leftarrow \mathsf{Gen}(1^n)$. Adversary gets oracles $\mathsf{Enc}(k,\cdot)$, $\mathsf{Dec}(k,\cdot)$; sends (m_0, m_1); receives c^*; may keep querying (but not c^* to Dec); sends b'. Win iff $b' = b$.

Definition 6 (CCA Security)

Π is **CCA-secure** if for all non-uniform PPT $\mathcal{A}$:

$$\mathsf{Adv}^{\mathsf{CCA}}_{\Pi,\mathcal{A}}(n) = \left| \Pr[\text{IND-CCA}_\Pi^\mathcal{A}(n) = 1] - \frac{1}{2} \right| = \mathsf{negl}(n)$$

Deterministic Encryption Cannot Be CPA-Secure

Theorem 7

No deterministic encryption scheme is CPA-secure.

Deterministic Encryption Cannot Be CPA-Secure

Theorem 7

No deterministic encryption scheme is CPA-secure.

Proof

Adversary queries $c = \mathsf{Enc}(k, m_0)$. Receives challenge $c^* = \mathsf{Enc}(k, m_b)$. If Enc is deterministic, $c^* = c$ iff $m_b = m_0$. So adversary outputs $b' = 0$ if $c^* = c$, else 1.

CPA-Secure Scheme from PRF

Theorem 8

If F is a PRF, then the following $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is CPA-secure for messages of length n.

Construction

- $\mathsf{Gen}(1^n)$: output $k \xleftarrow{\$} \{0,1\}^n$
- $\mathsf{Enc}(k, m)$: $r \xleftarrow{\$} \{0,1\}^n$; output $(r, F_k(r) \oplus m)$
- $\mathsf{Dec}(k, c = (c_1, c_2))$: output $c_2 \oplus F_k(c_1)$

Proof Sketch: CPA from PRF

Reduction

Assume $\mathcal{A}$ breaks CPA security of Π with advantage $\epsilon(n)$. Construct $\mathcal{B}$ breaking PRF F:

- $\mathcal{B}$ simulates CPA game for $\mathcal{A}$: on $\mathcal{A}$'s encryption query m, sample r, get y from F-oracle, return $(r, y \oplus m)$
- On challenge (m_0, m_1), $\mathcal{B}$ picks b, samples r^*, gets y^* from F-oracle, sends $c^* = (r^*, y^* \oplus m_b)$ to $\mathcal{A}$
- $\mathcal{B}$ outputs what $\mathcal{A}$ outputs

Proof Sketch: CPA from PRF

Reduction

Assume $\mathcal{A}$ breaks CPA security of Π with advantage $\epsilon(n)$. Construct $\mathcal{B}$ breaking PRF F:

- $\mathcal{B}$ simulates CPA game for $\mathcal{A}$: on $\mathcal{A}$'s encryption query m, sample r, get y from F-oracle, return $(r, y \oplus m)$
- On challenge (m_0, m_1), $\mathcal{B}$ picks b, samples r^*, gets y^* from F-oracle, sends $c^* = (r^*, y^* \oplus m_b)$ to $\mathcal{A}$
- $\mathcal{B}$ outputs what $\mathcal{A}$ outputs

If oracle is F_k: view of $\mathcal{A}$ is as in real game $\Rightarrow$ advantage $\epsilon(n)$. If oracle is random R: y^* random $\Rightarrow$ c^* hides m_b; advantage $\leq q/2^n$. So $\mathcal{B}$'s advantage $\geq \epsilon(n) - q/2^n = \text{nonnegl}(n)$.

Counter Mode (CTR)

Encryption (multiple blocks)

For message $(m_1, \ldots, m_\ell)$ with each $m_i \in \{0,1\}^n$:

1. $r \xleftarrow{\$} \{0,1\}^n$
2. Output $c = \big(r,\ m_1 \oplus F_k(r+1),\ m_2 \oplus F_k(r+2),\ \ldots,\ m_\ell \oplus F_k(r+\ell)\big)$

Counter Mode (CTR)

Encryption (multiple blocks)

For message $(m_1, \ldots, m_\ell)$ with each $m_i \in \{0,1\}^n$:

1. $r \xleftarrow{\$} \{0,1\}^n$
2. Output $c = (r,\ m_1 \oplus F_k(r+1),\ m_2 \oplus F_k(r+2),\ \ldots,\ m_\ell \oplus F_k(r+\ell))$

Decryption

Parse $c = (r, c_1, \ldots, c_\ell)$. For $i = 1, \ldots, \ell$: $m_i = c_i \oplus F_k(r+i)$.

Probability of breaking (simplified): $\frac{2q(n)-1}{2^n} \cdot q(n)$. In practice we use block ciphers (e.g., AES).

Summary

- **Private-key encryption**: Gen, Enc, Dec; correctness and confidentiality (IND, CPA, CCA).
- **CPA from PRF**: $(r, F_k(r) \oplus m)$; counter mode for multiple blocks.